

REMARKS

Claims 29-48, 55 and 56 were pending prior to this Amendment. In the Office Action mailed June 26, 2008, the Examiner rejected the earlier presented claims under section 103 as being unpatentable over Aiello (US PG PUB 2004/0123139) in view of Harrison et al. (US 6691113) and further in view of Cheline (US PG PUB No. 2003/0041136).

No claim stands rejected under section 102 for anticipation, and no claim stands rejected under section 103 for obviousness based on fewer than three references.

In this Amendment, Applicants have amended the three independent claims (29, 42 and 55) to even further differentiate the claimed invention from the Aiello-Harrison-Cheline combination that in the Examiner's view prevented patentability of the earlier presented claims.

First, Applicants have amended the claims to clarify that in Applicants' claimed invention malicious code written to temporary memory while permitting VPN access is eradicated from the end system in response to termination of the VPN connection. These amendments have support at, for example, p.3, lines 12-15, p.5, lines 2-7 and p.10, lines 20-22 and p.12, lines 7-10 of the original specification.

Second, Applicants have amended the claims to clarify that in Applicants' claimed invention filtering of non-VPN traffic is done on the end system. These amendments have support at, for example, p.4, lines 1 and 2, p.10, lines 3-10 and p.12, lines 2-6 of the original specification.

Applicants respectfully submit that the claims are in condition for allowance based on these amendments and the following considerations.

1. The Claims Are Allowable Since the Aiello-Harrison-Cheline Combination Does Not Teach or Suggest Purging Temporary Memory on the End System in Response to Detected Termination of the VPN Connection Whereby Malicious Code Written to Temporary Memory While Permitting VPN Access is Eradicated from the End System

One significant advantage of Applicant's invention resides in eliminating the risk of reinfection of a VPN network by an infected end system that is neglected during cleanup of the VPN network. This important security enhancement is achieved by limiting a VPN-connected end system's network connectivity strictly to the VPN and eradicating from the end system any malicious code acquired in a VPN session upon termination of VPN access. As stated in the Summary of the Invention at p.4, line 15 to p.5 line 7:

[S]ince the end system's network connectivity is strictly limited to the VPN, the end system is protected from infections that might otherwise be acquired in personal sessions. The end system's temporary memory can still be infected by malicious code during a session with in the VPN. And the end system can still spread such an infection to other resources within the corporate network during the session within the VPN. *However, damage is containable since the end system cannot transmit the malicious code outside the VPN, and since the temporary memory is purged when the VPN connection is terminated. Thus, the corporate network administrator can eradicate the malicious code altogether by shutting down the VPN, which ensures that the malicious code is removed from all remote thin client end systems, and cleaning up the corporate network. The risk of reinfection by remote end systems neglected in the cleanup effort is eliminated. (emphasis added).*

Stated differently, Applicants' invention recognizes that if malicious code is not allowed to persist on an end system after a VPN session, the end system cannot reinfect the VPN network in a later VPN session. This notable goal of Applicants' invention is manifest in the preamble of independent claim 29, which recites "A method for reducing vulnerability of a Virtual Private Network (VPN) protected network to attack by an end system"

Aiello, Harrison and Cheline express no concern for eliminating the risk of reinfection of a VPN network by an infected end system after VPN network cleanup, and the combination would not prevent such reinfection. Of the three references, Harrison is the one that the Examiner asserts discloses quarantining of untrusted data writes in a manner similar to Applicants' invention. However, Harrison's system does not operate in a VPN environment. And even if it did, Harrison's system still would not eliminate the risk of reinfection of a VPN network because instead of removing untrusted data from a client computer 100 at the end of a session, Harrison commits untrusted data to nonvolatile storage on client computer 100 for subsequent recall and use. Thus, any malicious code within the untrusted data may later infect or reinfect a network, a result that is antithetical to the teachings of Applicants' invention and the amended claims.

With this background in mind, we turn to the language of the claims--all of which as amended include or incorporate a limitation that addresses continuous monitoring on the end system for termination of the VPN connection and purging temporary memory on the end system in response to detected termination of the VPN connection whereby malicious code written to temporary memory while permitting VPN access is eradicated from the end system. The Aiello-Harrison-Cheline combination fails to teach or suggest this limitation.

The Examiner cites Harrison for alleged disclosure of preventing detected attempted writes to permanent memory while VPN access is permitted and purging temporary memory when VPN access is terminated. However, Harrison does not teach or suggest the above limitation in the claims as amended for at least two reasons. First, Harrison's system does not take action in response to termination of a VPN connection because Harrison's system is not deployed in a VPN setting. Harrison does not even mention VPNs. As Harrison is devoid of any VPN discussion, Harrison naturally does not make reference to taking action in response to termination of a VPN connection as recited in the claims as amended.

Second, Harrison does not disclose *purging temporary memory on an end system whereby malicious code written to temporary memory while permitting VPN access is eradicated from the end system*. Quite the contrary, Harrison instructs to preserve untrusted data at the end of an applet session by committing the untrusted data to nonvolatile disk storage 203 on client computer 100. More particularly, in Harrison an untrusted applet 304 downloaded from a Web server 120 is allowed to run in a restricted environment called a "sandbox" on client computer 100 and is allowed to write untrusted data to a repository 302 on client computer 100 while being prohibited from writing to the full client file system. (e.g. col. 7, lines 37-54). When untrusted applet 304 is thereafter unloaded, terminated or suspended, such as when client computer 100 is shut-down, repository 302 is automatically committed to nonvolatile disk storage 203 on client computer 100. (e.g. col. 5, lines 31-34, col. 7, lines 63-64, col. 9, lines 52-57). Any malicious code within the untrusted data written to repository 302 by untrusted applet 304 during an applet session is therefore saved on client computer 100 at the end of the session and may later infect or reinfect the network. This result is consistent with Harrison's goal of ensuring the integrity of a client computer, but is inconsistent with Applicants' goal of ensuring the integrity of a VPN network.

Accordingly, the claims as amended are allowable for at least the reason that the Aiello-Harrison-Cheline combination does not teach or suggest purging temporary memory on an end system in response to detected termination of a VPN connection whereby malicious code written to temporary memory while permitting VPN access is eradicated from the end system.

2. The Claims Are Allowable For the Further Reason that the Aiello-Harrison-Cheline Combination Does Not Teach or Suggest Filtering Detected Traffic Received on the End System that Is Not on the VPN Connection

Applicants have amended the claims to make clear that in Applicants' invention as claimed non-VPN traffic is filtered *on the end system*. Aiello is the reference in the Aiello-Harrison-Cheline combination that in the Examiner's view teaches filtering detected traffic inbound to the end system that is not on the VPN connection. There is no indication in Aiello, however, that non-VPN traffic is filtered on the end system. Aiello discloses a filter module 112, 508 in an ISP network 110, 506 that filters non-VPN packets received on a VPN tunnel. As is well-known, an ISP network includes transit devices, such as routers, switches and bridges, which are not end systems.

In the event some of the non-VPN packets inadvertently "leak through" filter module 112, 508 in ISP network 110, 506, Aiello further discloses a monitor module 504 that may reside on a mobile station 500 that detects the non-VPN packets and sends out alerts so that appropriate action can be taken, such as terminating the VPN tunnel. While monitor module 504 detects non-VPN packets, however, there is no suggestion that monitor module 504 *filters* non-VPN packets. Thus, there is no teaching in Aiello to filter non-VPN packets on an end system.

Accordingly, the claims as amended are allowable for the further reason that the Aiello-Harrison-Cheline combination does not teach or suggest filtering detected traffic received on the end system that is not on the VPN connection.

3. Claims 55 and 56 Are Allowable for the Further Reason that the Aiello-Harrison-Cheline Combination Does Not Teach or Suggest a Plurality of Memories "Consisting of" at Least One Write-Protected Permanent Memory and at Least One Temporary Memory

Claim 55 recites a VPN-capable end system having a plurality of memories consisting of at least one write-protected permanent memory and at least one temporary memory. According to accepted patent examining procedures, use of the transitional phrase "consisting of" in claim 55 means that the *entire* permanent memory on the VPN-capable end system recited in claim 55 is write-protected. See MPEP 2111.03.

Cheline is the reference in the Aiello-Harrison-Cheline combination that the Examiner relies on as disclosing a plurality of memories consisting of at least one write-protected permanent memory and at least one temporary memory. However, in contrast to what is recited, Cheline allows writing of a permanent memory (flash memory 234) by both client- and server-side systems. For example, at paragraph [0057] of Cheline it is stated: "The flash memory 234 is a type of constantly-powered nonvolatile memory that can be erased and reprogrammed in units of memory called blocks." Thereafter, multiple instances of writing the flash memory by a client computer and VPN service provider are described. At paragraph [0063] of Cheline, it is indicated that the user of one of client computers and the modem receive from a VPN service provider a one-time only password that is stored in the flash memory. At paragraph [0064] of Cheline, it is indicated that the modem further receives from a VPN service provider VPN security policies, a private key and certificate, and a root CA certificate that are

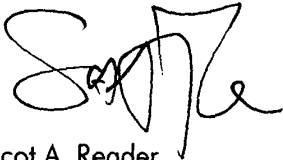
stored in the flash memory. And at paragraph [0067] of Cheline, it is indicated that the modem receives from a client computer upon requesting initiation of a VPN session a MAC address and/or IP address that is/are stored in the flash memory. Cheline's teaching to allow permanent memory to be written renders its VPN platform vulnerable to permanent infection and teaches away from what is recited in claim 55.

Accordingly, claims 55 and 56 are allowable for the further reason that the Aiello-Harrison-Cheline combination does not teach or suggest a VPN-capable end system having a plurality of memories consisting of at least one write-protected permanent memory and at least one temporary memory.

In view of the foregoing, consideration and favorable action on all claims are respectfully requested. Accordingly, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Should any question remain in view of this communication, the Examiner is encouraged to call the undersigned so that a prompt disposition of this application can be achieved.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Scot A. Reader', with a stylized flourish at the end.

Scot A. Reader
Reg. Number 39,002
Tel. No. (303) 440-4050
Scot A. Reader, P.C.
1320 Pearl Street, Suite 228
Boulder, CO 80302